

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-044354

(43)Date of publication of application : 14.02.1997

(51)Int.Cl.

G06F 9/06
G06F 1/00
G06F 13/00
G09C 1/00
H04L 9/32
H04N 7/167

(21)Application number : 07-212633

(71)Applicant : SONY CORP

(22)Date of filing : 28.07.1995

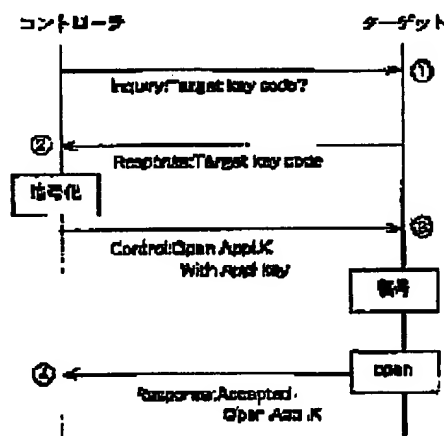
(72)Inventor : KAWAMURA HARUMI

(54) ELECTRONIC APPARATUS AND ITS OPERATION CONTROL METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To enable other companies to use each independently developed application by transmitting a control signal, which includes preliminarily determined cipher information and has a prescribed format, from an apparatus on the control side and setting the application to the executable state by an apparatus on the controlled side in the case of reception of the control signal including preliminarily determined cipher information.

SOLUTION: When receiving a target key code from a target (2), a controller multiplies a cipher function by this target key code to calculate an application key code. An open command of the application to which the application number and the calculated application key code are added is transmitted to the target (3). The target confirms whether the decoded result is equal to its own target key code or not; and if it is equal, the target validates the open command of the application K and enters into the open state that the application can be executed.



LEGAL STATUS

[Date of request for examination]

29.07.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-44354

(43) 公開日 平成9年(1997)2月14日

(51) Int.Cl. ⁴	識別記号	序内整理番号	F I	技術表示箇所
G 0 6 F 9/06	5 5 0		G 0 6 F 9/06	5 5 0 G
	1/00	3 7 0		3 7 0 E
	13/00	3 5 1		3 5 1 F
G 0 9 C 1/00	6 6 0	9460-5E	G 0 9 C 1/00	6 6 0 D
H 0 4 L 9/32		7259-5J	H 0 4 L 9/00	6 7 3 Z
審査請求 未請求 請求項の数9 FD (全 10 頁) 最終頁に続く				

(21) 出願番号 特願平7-212633

(22) 出願日 平成7年(1995)7月28日

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 川村 晴美

東京都品川区北品川6丁目7番35号 ソニー株式会社内

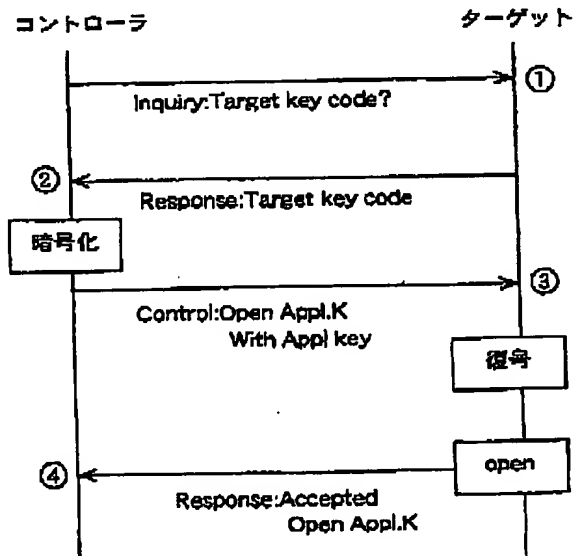
(74) 代理人 弁理士 杉山 猛

(54) 【発明の名称】 電子機器及びその動作制御方法

(57) 【要約】

【課題】 IEEE-1394のベンダーユニークコマンドを用いて独自に開発したアプリケーション毎に他社による使用を可能にする。

【解決手段】 コントローラは、ターゲットキーコードを受けとると(手順②)、暗号関数とそのターゲットキーコードとから、アプリケーションキーコードを算出する。そして、アプリケーションキーコードを付けたアプリケーションのオープンコマンドを送信する(手順③)。ターゲットはオープンコマンドを受信したら、コマンド中のターゲットキーコードを復号する。そして、復号した結果が自分のターゲットキーコードと等しければ、アプリケーションを実行可能なオープン状態にする。



【特許請求の範囲】

【請求項1】 複数の電子機器をバスで接続し、該電子機器間で情報信号及び制御信号の通信を行なうシステムにおいて、電子機器の製造元情報を含む所定のフォーマットの制御信号を用いて実現したアプリケーションの動作を制御する方法であって、制御する側の電子機器は制御される側の電子機器に対してあらかじめ定められた暗号情報を含む前記所定のフォーマットの制御信号を送信し、該制御される側の電子機器は受信した制御信号にあらかじめ定められた暗号情報が含まれているときに、前記アプリケーションを実行可能状態にすることを特徴とする電子機器の動作制御方法。

【請求項2】 暗号情報は電子機器毎に定められているキーコードとアプリケーション毎に定められている暗号関数とから作成されるものである請求項1記載の電子機器の動作制御方法。

【請求項3】 制御する側の電子機器は制御される側の電子機器に対してキーコードを問い合わせ、該制御される側の電子機器から返答されたキーコードとあらかじめ自分が保持している暗号関数とから暗号情報を作成し、該暗号情報を前記制御される側の電子機器へ送信する請求項2記載の電子機器の動作制御方法。

【請求項4】 制御される側の電子機器は誤った暗号情報を受信してアプリケーションを実行可能状態にしなかったときに、アプリケーションを実行可能状態にしたことを制御する側の電子機器に知らせる請求項1記載の電子機器の動作制御方法。

【請求項5】 制御する側の電子機器は制御される側の電子機器に対して製造元情報を問い合わせ、該制御される側の電子機器から返答された製造元情報があらかじめ自分が保持しているリストに登録されているかどうかを判定し、登録されていないときは、アプリケーションを実行可能状態にする手順を実行しない請求項1記載の電子機器のアプリケーションの動作制御方法。

【請求項6】 キーコードをあらかじめ定められた期間毎に変化させる請求項2記載の電子機器の動作制御方法。

【請求項7】 キーコードをあらかじめ定められた生産台数毎に変化させる請求項2記載の電子機器の動作制御方法。

【請求項8】 キーコードと暗号情報とを1対1に割り付けた請求項2記載の電子機器の動作制御方法。

【請求項9】 複数の電子機器をバスで接続し、該電子機器間で情報信号及び制御信号の通信を行なうシステムにおける電子機器であって、電子機器の製造元を示す識別情報を含む所定のフォーマットの制御信号を用いて実現したアプリケーションを有し、あらかじめ定められた暗号情報が含まれている所定のフォーマットの制御信号により前記アプリケーション

を実行可能状態にすることを特徴とする電子機器。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明は複数の電子機器をバスで接続し、それらの電子機器間で通信を行なうシステムに関し、より詳細には独自に開発したアプリケーションをライセンス契約して他社でも使用可能とするためのシステムに関する。

【0002】

【従来の技術】 複数の電子機器をバスで接続し、それらの電子機器間で通信を行なうシステムとしては、IEEE-1394シリアルバスを用いた通信システムが考えられている。IEEE-1394シリアルバスを用いた通信システムは、デジタルビデオテープレコーダ、デジタルビデオカメラ、デジタルテレビジョン受像機、パーソナルコンピュータ等の電子機器（以下機器と略す）をIEEE-1394シリアルバスで接続し、それらの機器間でデジタルオーディオ/ビデオ信号等の情報信号や接続制御コマンド等の制御信号の通信を行なうものである。

【0003】 IEEE-1394シリアルバスを用いた通信システムでは、各メーカーが独自のアプリケーションを実現するためにベンダーユニークコマンド（Vendor Unique Command）が用意されている（各社で互換性をとるべき基本的なコマンドはベンダーユニークコマンドとは別に定義されている。）。ベンダーユニークコマンドのパケットには、そのメーカーであることを示すカンパニーIDを付けることになっている。したがって、基本的にベンダーユニークコマンドを用いて実現するアプリケーションは、そのメーカー1社でのみ有効となるものである。

【0004】

【発明が解決しようとする課題】 独自に開発されたアプリケーションであっても他社に有効な場合がある。そのアプリケーションが共通コマンドとして登録するほどの汎用性がない場合には、あるメーカーが開発したアプリケーション用のコマンドを他のメーカーでも使用したいことがある。他のメーカーがそのアプリケーション用のベンダーユニークコマンドを使用するには、アプリケーションを開発したメーカーのカンパニーIDを使用しなければならない。

【0005】 そこで、アプリケーションを開発したメーカーが正式にライセンス契約をして他のメーカーにカンパニーIDの使用を認めたとすると、そのアプリケーション以外のベンダーユニークコマンドまでもが他社でも使用できてしまう。

【0006】 本発明はこのような問題点に鑑みてなされたものであって、独自に開発したアプリケーション毎に他社による使用を可能にする機器及びその制御方法を提供するものである。

【0007】

【課題を解決するための手段】前記課題を解決するために、本発明に係る機器及びその動作制御方法は、複数の機器をバスで接続し、これらの機器間で情報信号及び制御信号の通信を行なうシステムにおいて、機器の製造元を示す識別情報を含む所定のフォーマットの制御信号を用いて実現したアプリケーションの動作を制御する方法であって、制御する側の機器は制御される側の機器に対してあらかじめ定められた暗号情報を含む前記所定のフォーマットの制御信号を送信し、制御される側の機器は受信した制御信号にあらかじめ定められた暗号情報が含まれているときに、前記アプリケーションを実行可能状態にすることを特徴とするものである。

【0008】本発明によれば、制御する側の機器は制御される側の機器に対してあらかじめ定められた暗号情報を含む前記所定のフォーマットの制御信号を送信し、制御される側の機器は受信した制御信号にあらかじめ定められた暗号情報が含まれているときに、前記アプリケーションを実行可能状態にする。

【0009】

【発明の実施の形態】以下本発明の実施の形態について、

【1】ベンダーユニークコマンド (Vendor Unique Command)

【2】ベンダーユニークコマンドの他社での使用

【0010】【3】システムの内容説明

【3-1】アプリケーションのオープン

【3-2】暗号化の条件

【3-3】アプリケーションのオープンに必要な情報

【3-4】アプリケーションのオープンの方法

【3-5】オープン中のコマンド

【3-6】アプリケーションのクローズ

【3-7】アプリケーション実行およびクローズの条件

【0011】【4】アプリケーションの保護

【4-1】カンパニーIDによる管理

【4-2】ターゲットキーコードの設定

【4-3】暗号関数fk

【0012】【5】ターゲットの構成と動作

の順序で詳細に説明する。

【0013】【1】ベンダーユニークコマンド (Vendor Unique Command)

IEEE-1394シリアルバスに対するデジタルインターフェイスの機能制御プロトコル (Function Control Protocol: 以下FCPと略す) では、複数のコマンドトランザクションセット (Command Transaction Set) を使用することができる。

【0014】図1にベンダーユニークフレームのフォーマットを示す。ここで、OTS (Command Transaction Set) = 1110がベンダーユニークフレームであることを示す。そして、CTSの次に4ビットを空けて、3バイトのベンダーID (IEEEで定められたカンパニーID) を用いる。ベンダーユニークであることを示すCTSとベンダーID以外はベンダーが自由に定義し、使用することができる。つまり、そこで使用するコマンドセットもコマンド/レスポンスの送受信等のトランザクションについてもベンダーに依存することとなっている。なお、ゼロパッドバイト (zero pad bytes) は、フレームの長さを4バイト (クアドレット) 単位にするために必要に応じて設けられる。

【0015】図2にAV機器制御用のコマンドトランザクションセットであるAV/C (Audio Visual Control) コマンドトランザクションセットのフレーム構成を示す。ここで、CTS=0000がAV/Cコマンドトランザクションセットであることを示す。

【0016】AV/Cコマンドトランザクションセットでも、ベンダーが自由にコマンドを定義することができるようにオペコード (OPC) としてベンダーユニークが定義されている。ただしコマンド/レスポンスのトランザクションについてはAV/Cコマンドトランザクションセットに従う。この場合のフレーム構成を図3に示す。OPC=00hでベンダーユニークであることを表す。ベンダーIDは前記の場合と同様、3バイトのカンパニーIDを用いる。

【0017】【2】ベンダーユニークコマンドの他社での使用
FCPでは他のノードを制御するノードのことをコントローラ、制御される側のノードをターゲットと呼ぶ。以下コントローラ、ターゲットという名称を用いて説明する。

【0018】ベンダーユニークコマンドはベンダーIDに記されたカンパニーIDを所有している会社が定義し、使用するものであるが、アプリケーションによっては他の会社も同じコマンドを使用したい場合も出てくる。

【0019】ここではカンパニーID=xxxxxxhのA社と、カンパニーID=yyyyyyhのB社を例に説明する。A社はアプリケーションKの独自のコマンドをベンダーユニークコマンドとして定義し、A社の製品で使用している。B社はA社のこのベンダーユニークコマンドを用いたアプリケーションKをB社の製品でも対応したいと考えた。B社での対応の方法としては2つの場合がある。B社がコントローラを製造しA社の製品をターゲットとして制御する場合と、B社がターゲットとなる製品を作りA社のコントローラで制御されるようにする場合である。どちらの場合でもA社のベンダーユニークコマンドを使用しなければアプリケーションKの実現はできない。

【0020】以下に説明するシステムは、ベンダーユニークコマンドの所有者である会社がベンダーユニークコマンドを用いて実現したアプリケーションのうち幾つかについては、限定した会社での使用を可能とするためのものである。

【0021】このシステムを導入することによって、一般的にはベンダーユニークコマンドの他社での使用を禁止とするが、アプリケーション毎に使用権を与えるようにすることが可能となる。したがって前記の場合のB社もA社のアプリケーションKに関してはベンダーユニークコマンドを使用することができるようになる。

【0022】〔3〕システムの内容説明

(3-1) アプリケーションのオープン

ターゲットはベンダーユニークコマンドにより実現するアプリケーション毎に、「オープン状態」「クローズ状態」を有する。オープン状態とはコマンドを受けて、そのアプリケーションを実行することが可能な状態である。クローズ状態とは、コマンドを受けたとしても実行しない状態である。

【0023】前記のようにベンダーユニークコマンドは一般に公開しているコマンドではないので、第三者(C社とする)が勝手にA社のカンパニーID= $x \times x \times x \times h$ を付けてコマンドを送った場合にコマンドが実行されないようにするため、通常はアプリケーションを全てクローズ状態にしておく。そして、ベンダーユニークコマンドを定義したA社はもとより、使用権を得たB社についても、該当するアプリケーションKをオープン状態にしてからアプリケーションKを実行することとした。このとき、オープン状態にするための手段を教えることがそのアプリケーションの使用権を与えることに等しい。

【0024】(3-2) 暗号化の条件

コントローラはターゲットに対して、オープン状態にしたいアプリケーションを指定してオープンコマンドを送る。この時、コントローラとターゲットの間で取り決めた交換しておき、決められたコードを付けてオープンコマンドが送られた場合のみ有効とする。このコードは第三者にはわからないようにする必要がある。このコードは、あらかじめA社とB社との間で決めておく。そのとき、各機器毎あるいは1つの機器でも時間によって異なる値にするなどの対応をとる。

【0025】このコードは一種の暗号と考えられるが、コンシューマ機器での使用を目的とするので、1チップマイクロコンピュータでも簡単に対応できるようにし、コントローラ、ターゲット共に負担をできるだけ軽くする必要がある。コンシューマ機器では商品が一度市場に出たならば、その後暗号の方式を変えることは困難である。

【0026】(3-3) アプリケーションのオープンに必要な情報

各アプリケーションをオープンさせる際に必要な情報について説明する。

(1) アプリケーションナンバー (Application No)

アプリケーションの種別をあらわすコードをアプリケーションナンバーと呼ぶことにする。図4にアプリケーションナンバーの例を示す。ここでは、1バイトでアプリケーションの種別を表している。アプリケーションナンバーを01hからFEhまで割り当て可能とすると、254種類のアプリケーションまで対応できる。00hは各アプリケーションに共通に用いるために使用禁止(reserved)としておく。また、アプリケーションの数が増えた時のために、FFhは拡張用としてreservedとしておく。

【0027】(2) 暗号関数f

アプリケーションをオープンさせる際にアプリケーションナンバーとともに送る「鍵」をアプリケーションキーコードと呼ぶ。アプリケーションキーコードの生成方法(暗号化)はアプリケーション毎に異なり、あらかじめA社、B社間で決めておく。これを暗号関数fとし、アプリケーションKの暗号関数をfkとする。

【0028】(3) ターゲットキーコード

ターゲットキーコードはターゲット毎に定める値であり、全てのアプリケーションに対してアプリケーションキーコードの生成の元となるものである。そして、機器毎に異なるターゲットキーコードを付ける等の対応によって、1つのアプリケーションでもアプリケーションキーコードを変える。

【0029】アプリケーションのオープンの際には、コントローラはターゲットにターゲットキーコードの問い合わせ命令を送り、返答を得ることにより、その時のターゲットキーコードを知る。

【0030】(4) アプリケーションキーコード

ターゲットキーコードを暗号関数fで暗号化したものがアプリケーションキーコードとなる。つまり、アプリケーションKに対するアプリケーションキーコードはアプリケーションキーコード= $f k$ (ターゲットキーコード)と表せる。

【0031】(3-4) アプリケーションのオープンの方法

コントローラがターゲットのアプリケーションKをオープン状態にする方法について説明する。

【0032】(1) コマンド送信手順

図5にコントローラ/ターゲット間のコマンド/レスポンスの概略図を示す。まず、コントローラはターゲットに対し、ターゲットキーコードの問い合わせコマンドを送信する(手順①)。ターゲットはそれに対するレスポンスとして、その時の自分のターゲットキーコードを返信する(手順②)。

【0033】コントローラは、ターゲットキーコードを受けると、暗号関数 f_k にそのターゲットキーコードをかけ、アプリケーションキーコードを算出する。次に、コントローラはターゲットに対し、アプリケーションNoと算出したアプリケーションキーコードを付けて、アプリケーションのオープンコマンドを送信する（手順③）。

【0034】ターゲットはオープンコマンドを受信したら、指定されたアプリケーションNoのアプリケーションを備えているかどうかを確認する。そして、対応しているアプリケーションの場合、受信したアプリケーションキーコードをその暗号関数 f_k の逆関数にかけ、復号する。

【0035】ターゲットは復号した結果が自分のターゲットキーコードと等しいかどうかを確認する。そして、等しい場合に初めてアプリケーションKのオープンコマンドを有効とし、アプリケーション実行可能なオープン状態に入る。

【0036】ターゲットはアプリケーションKをオープン状態にしたら、コントローラに対して、アプリケーションKをオープン状態にしたこと知らせるためのレスポンスを返す（手順④）。

【0037】（2）コマンドフォーマット

図1と図3を参照しながら説明したように、ベンダーユニークコマンドは、ベンダーユニークフレーム又はAV/Cコマンドトランザクションセットのいずれを用いても実現できるが、ここでは、コマンド構成として、AV/Cコマンドトランザクションセットを用いた場合の例を示す。

【0038】図6にベンダーユニークコマンドの構成を示す。ここでは3バイトのベンダーIDに続くベンダーが独自に定義する領域（OPR4以降）のみ図示した。前述したように、コマンド/レスポンスのトランザクションについてはAV/Cコマンドトランザクションセットに準ずるものとする。アプリケーションを実行する具体的なコマンドについてはここで記載しない。これは各アプリケーション毎に定義する。

【0039】図7にターゲットキーコードの問い合わせのコマンド/レスポンスを示す。ここではアプリケーションNoを $k k h$ 、ターゲットキーコードを16ビットの $1 2 3 4 h$ とした。なお、ターゲットキーコードの長さはアプリケーション毎に定めることができる。

【0040】ターゲットキーコードは機器毎/アプリケーション毎に異なる値としたり、乱数とすることも考えられるので、各アプリケーションを実行開始する際には必ず問い合わせをする。図7（a）は問い合わせのコマンドを示す。ここでOPR4はアプリケーションNoであり、OP5の $1 0 h$ とOP6の $7 1 h$ でターゲットキーコードの問い合わせであることを示す。また、OP7とOP8は $F F h$ （ダミー）とする。

【0041】ターゲットは、問い合わせのコマンドに付いているアプリケーション（アプリケーションK）に対応している場合には、図7（b）に示すように、OP7とOP8に16ビットのターゲットキーコード $1 2 3 4 h$ を付けた“Stable”のレスポンスをコントローラに返答する。そのアプリケーションに対応していない場合には、図7（c）に示すように、問い合わせコマンドと同じ内容の“Not Implemented”のレスポンスを返す。

【0042】次に、コントローラがターゲットに送るアプリケーションKのオープンコントロールコマンドおよびそのレスポンスを図8（a）、（b）に示す。ここではアプリケーションキーコードを16ビットの $5 6 7 8 h$ とした。なお、アプリケーションキーコードの長さはアプリケーション毎に定めることができる。

【0043】コマンドに付いているアプリケーションキーコードの指定値がターゲットが持っているアプリケーションキーコードの値と異なっていてオープンできない場合には、コントローラに対して“Rejected”のレスポンスを返すのが基本である。しかし、第三者がアプリケーションキーコード探し求める過程においては、 $0 0 0 0 h$ から $F F F F h$ まで1つずつ試してみることが考えられる。そこでオープンできなかった場合でもわざと“Accepted”のレスポンスを返答する。図8（c）、（d）にオープンできない場合の例（正しいアプリケーションキーコード $= 5 6 7 8 h$ のところ、 $5 6 7 9 h$ を指定）を示す。第三者はオープンコマンドのトランザクションだけではオープンに成功したかどうか分からないので、アプリケーションの実行コマンドを送ってみるか、オープン中かどうか問い合わせで調べるという手順が必要となる。

【0044】アプリケーションがオープン状態であるかクローズ状態であるかの問い合わせもアプリケーションキーコードを付けて送る。アプリケーションキーコードの指定値が正しい場合には“Accepted”を、異なっている場合には“Rejected”をレスポンスとして返す。図9（a）、（b）にアプリケーションキーコードとして正しい値（ $5 6 7 8 h$ ）を指定された場合のコマンドとレスポンスの例を示す。

【0045】（3-5）オープン中のコマンド
アプリケーションがオープン（実行可能状態）している間のみ、ターゲットはそのアプリケーション用のコマンドを受け付ける。コマンドフォーマットとしては図6のように最初の1バイトでアプリケーションNoを示す他は、各アプリケーション毎に定める。

【0046】アプリケーションがオープン状態であるか、クローズ状態であるかにかかわらず、対応していないアプリケーションの実行コマンドを受けた場合にはレスポンスとしては“Not Implemented”を返す。また、アプリケーションがオープン状態であっ

ても、アプリケーション毎に定めたO P Oとして指定されたものに対応していない場合には、レスポンスとしては“Not Implemented”を返す。

【0047】(3-6)アプリケーションのクローズターゲットとなる機器は電源をオフにする際に基本的に全てのアプリケーションを自動的にクローズ状態にする。再び電源が入れた場合にもクローズ状態を継続する。

【0048】コントローラはアプリケーションの実行を終了した際に、ターゲットにクローズコマンドを送信する。図10にクローズコマンドの例を示す。このように、クローズの際にもアプリケーションキーコードを付けてコマンドを送る。ターゲットはクローズコマンドを受けると、そのクローズコマンドのアプリケーションNoに示されるアプリケーションをクローズ状態にする。このとき、アプリケーションキーコードの値が異なってもクローズ状態にする。本システムでは通常はアプリケーションはクローズ状態とし、実行させる際のみにオープンさせることが基本である。

【0049】なお、オープン状態ならば受け付けるコマンドをクローズ状態で受けた場合には、レスポンスとしては“Rejected”を返す。

【0050】(3-7)アプリケーション実行およびクローズの条件

アプリケーションによっては長時間オープンのままでは問題が生じるものや、一度オープンさせたら独占的に制御を行ないたいものなど、様々な場合が考えられる。したがって、アプリケーション毎にその用途に適した実行条件等を定めるものとする。以下にその例を記す。

【0051】(1) オープン時間の制限
オープン状態にいるにもかかわらず、そのアプリケーション実行のためのコマンドが一定時間以上アクセスされない場合には、強制的にクローズする。タイムアウトの時間についてはアプリケーション毎に定める。

【0052】(2) バスの異常処理
バスにリセットがかかった場合には、強制的にクローズする。

【0053】(3) アプリケーション実行許可台数
複数のコントローラからの制御を許可しないようにする。ターゲットはそのアプリケーションをオープンしたコントローラを記憶しておき、アプリケーション実行コマンドについてはそのコントローラからのコマンドのみ受けけるようにする。このとき、オープン中であっても他のコントローラからのコマンドはRejectする。複数のコントローラからの制御を許可するが、その台数を限定してもよい。

【0054】(4) アプリケーションの保護
暗号化したアプリケーションキーコードを送るからといっても、そのアプリケーションを完璧に保護したことはない。このアプリケーションの使用権を持たない

第三者であっても、コントローラとターゲットの間の通信内容は傍受できるので、傍受したターゲットキーコードとアプリケーションキーコードからコンピュータを用いて暗号関数f kを求めることが考えられるからである。

【0055】(4-1) カンパニーIDによる管理
そこで、このような事態に対してアプリケーションを保護する手段を考えた。使用権を持たない第三者がターゲットとなる機器を作った場合、コントローラ側の負荷を無視すれば、以下のような方法で第三者の検出を行ないアプリケーションを実行させないことが可能である。

【0056】パーソナルコンピュータがコントローラとなり、アプリケーションを実行させるような場合の例を説明する。パーソナルコンピュータにアプリケーション実行の対象となる会社(使用権を持っている会社)のカンパニーIDを登録しておく。そして、ターゲットにベンダーIDの問い合わせコマンドを送り、そのレスポンスに付けられたベンダーIDが登録されているかどうかを調べる。IEEE-1394シリアルバスに対応する機器は、内部にノードユニークIDが書き込まれているので、例えば図5の手順①より前にこの問い合わせを行なう。このとき、第三者であるC社(カンパニーID=zzzzzzzh)が、勝手にA社のベンダーID=xxxxxxhに基づくベンダーユニークコマンド受けアプリケーションKを実行できるように作ったとしても、コントローラは図11に示すような登録IDのリストを基に、C社が登録されていないことを知ることができるので、アプリケーションKを起動させないようにすることができる。

【0057】この場合、実際にはアプリケーションKの使用権を得る会社が増えることが考えられるので、上記例のような保護の仕方は、リストの更新が可能となるような場合に適用できるものである。

【0058】(4-2) ターゲットキーコードの設定
アプリケーションキーコード=f k (ターゲットキーコード)

の関係式では、ターゲットキーコード、アプリケーションキーコードのサンプル数が多いほど、暗号関数f kの解読は容易となる。コンシューマ機器での適用を考えると、ある機種においてターゲットキーコードが頻繁にはなくたまに変化することが望ましい。そこで、例えば以下のようにターゲットキーコードの設定を行なう。

【0059】(1) 生産台数での切替え

例えば10万台ごとにターゲットキーコードを切り替える。第三者がコントローラを作った場合、最初の10万台のターゲットキーコードには対応できても、その後生産されたものについては第三者の作ったコントローラでは動作しないことになる。

【0060】(2) 内蔵時計(カレンダー)での切替え
同一機器でも、例えば1年ごとにターゲットキーコード

を切り替える。1995年に生産された機器は1995をもとにした値をターゲットキーコードとする。第三者はこの初期のターゲットキーコードをもとにコントローラを作ることになる。したがって、当初は第三者のコントローラでも動作してしまうが、年が変わると動作しなくなる。

【0061】(4-3) 暗号関数 f_k

暗号関数 f_k が数値演算式の場合、ターゲットキーコード、アプリケーションキーコードのサンプル数によっては簡単に f_k を求めることができる。そこでコンシューマ機器への導入の際には、 f_k は数値関数とはせず、ターゲットキーコードに対してアプリケーションキーコードを1対1に割り付け、その対応表を f_k としてアプリケーションKの使用権を持つ会社にも渡すこととする。図12に対応表の例を示す。このようにすれば、暗号関数 f_k を求めることは困難になる。また、1チップマイクロコンピュータでも簡単に対応できる。さらに、商品が一度市場に出た後でも、ROMのバージョンアップにより比較的簡単に暗号の方式を変えることができる。

【0062】〔5〕ターゲットの構成

図13に本発明を適用したターゲットの構成の例を示す。この図に示すように、ターゲットとなるノードは、マイクロコンピュータ1と、ターゲットキーコードメモリ2と、暗号関数メモリ3と、時計4と、通信インターフェイス5とを備えている。

【0063】マイクロコンピュータ1は内蔵するアプリケーションのオープン/クローズ、コマンド/レスポンスの作成、アプリケーションキーコードの作成等、アプリケーションに関する処理の全てを司る。

【0064】ターゲットキーコードメモリ2は、アプリケーション毎に異なるターゲットキーコードを保持している。また、ここにはターゲットキーコードを1年毎に切り替えられるように、各アプリケーション毎に複数のターゲットキーコードが格納されている。

【0065】暗号関数メモリ3はアプリケーション毎の暗号関数 f_k を保持している。ここでは、図12のようなターゲットキーコードとアプリケーションキーコードとの対応表を記憶したROMテーブルである。

【0066】時計4は現在の時刻情報をマイクロコンピュータ1に知らせる。マイクロコンピュータ1はこの時刻情報を見て、年が変わるごとにターゲットキーコードを切り替えて読み出す。

【0067】通信インターフェイス5はIEEE-1394シリアルバス6に対してコマンド/レスポンスを送受信するためのインターフェイスである。なお、実際のターゲットにはオーディオ/ビデオ信号を処理するためのブロックが設けられているが、ここではアプリケーションのオープンに関連するブロックのみを示した。

【0068】ここでコントローラの構成について簡単に説明しておく。図13のターゲットに対応するコントロ

ーラは、マイクロコンピュータと、暗号関数メモリと、通信インターフェイスを備えている。もしコントローラが、(4-1)で説明したカンパニーIDによる管理を行なっているのであれば、さらにアプリケーション実行の対象となる会社カンパニーIDを登録しておくメモリを備えている。

【0069】次に図13に示したターゲットがアプリケーションをオープンにするまでの動作を説明する。まず、コントローラが送信したターゲットキーコードの問い合わせコマンドを受けとる(図5の手順①、図7

(a)を参照)。マイクロコンピュータ1はターゲットキーコードメモリ2を参照し、問い合わせコマンドに付いていたアプリケーションNoに対応するターゲットキーコードを読み出し、通信インターフェイス5を介して“Stable”のレスポンスを送信する(図5の手順②、図7(b)を参照)。問い合わせコマンドに付いていたアプリケーションNoに対応するターゲットキーコードが存在しない場合には、“Not Implemented”のレスポンスを送信する(図7(c)を参照)。

【0070】コントローラはターゲットから“Stable”のレスポンスを受けとると、そこに付いているターゲットキーコードを検出し、内蔵する暗号関数メモリを読み出してアプリケーションキーコードを作成する。この暗号関数メモリはターゲットの暗号関数メモリ3と同様に構成されている。コントローラは作成したアプリケーションキーコードを付けたオープンコマンドをターゲットに送信する。(図5の手順③、図8(a)を参照)。

【0071】ターゲット内のマイクロコンピュータ1は、受けとったオープンコマンドに付いていたアプリケーションキーコードと、自分の暗号関数メモリ3に格納されているターゲットキーコードに対応するアプリケーションキーコードとを比較する。すなわち、ここでは図5に示したように暗号関数の逆関数を用いてアプリケーションキーコードからターゲットキーコードを復号化するのではなく、コントローラと同様、暗号化を行なっているわけである。勿論、アプリケーションキーコードからターゲットキーコードを復号するように構成してもよい。比較したアプリケーションキーコード同士が一致していれば、アプリケーションをオープン状態にすると共に、コントローラに対して、アプリケーションをオープン状態にしたこと知らせるため“Accepted”のレスポンスを返す(図5の手順④を参照)。

【0072】

【発明の効果】以上詳細に説明したように、本発明によれば機器の製造元を示す識別情報を含む所定のフォーマットの制御信号を用いた独自のアプリケーションを他社でも使用することができ、かつアプリケーション毎に使用を許可/禁止することができる。そして、複雑な暗号

(8)

特開平9-44354

化等を用いずにアプリケーションの保護が可能となる。

【図面の簡単な説明】

【図1】ベンダーユニークフレームのフォーマットを示す図である。

【図2】AV/Cコマンドトランザクションセットのフレーム構成を示す図である。

【図3】AV/Cコマンドトランザクションセットで定義されているベンダーユニークフレームの構成を示す図である。

【図4】アプリケーションナンバーの例を示す図である。

【図5】コントローラ/ターゲット間のコマンド/レスポンスの概略を示す図である。

【図6】ベンダーユニークコマンドの構成を示す図である。

【図7】ターゲットキーコードの問い合わせのコマンド

/レスポンスを示す図である。

【図8】アプリケーションKのオープンコントロールコマンド/レスポンスを示す図である。

【図9】アプリケーションキーコードとして正しい値を指定された場合のオープン/クローズ問い合わせコマンド/レスポンスの例を示す図である。

【図10】クローズコマンドの例を示す図である。

【図11】使用権を持っている会社のカンパニーIDの登録リストの例を示す図である。

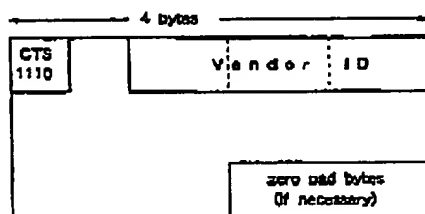
【図12】ターゲットキーコードとアプリケーションキーコードの対応表の例を示す図である。

【図13】ターゲットの構成の例を示す図である。

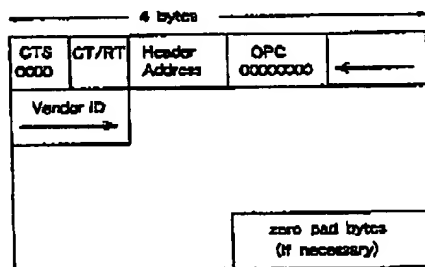
【符号の説明】

1…マイクロコンピュータ、2…ターゲットキーコードメモリ、3…暗号関数メモリ、4…時計、5…通信インターフェイス、6…IEEE-1394シリアルバス

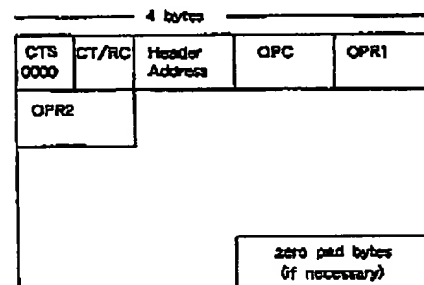
【図1】



【図3】



【図2】



CTS:コマンドトランザクションセット

CT/RC:コマンドタイプ/レスポンスタイプ

Header Address:コマンドの宛先、レスポンスの発信元のサブデバイス(あるいはデバイス)

OPC:オペコード

OPR:オペランド

【図4】

Application No	アプリケーションの種類
00 h	(使用禁止)
01 h	VCR制御 (基本)
02 h	VCR制御 (特殊)
03 h	チューナー制御
10 h	...
11 h	...
12 h	...
13 h	...
14 h	...
15 h	...
16 h	...
17 h	...
18 h	...
19 h	...
1A h	...
1B h	...
1C h	...
1D h	...
1E h	...
1F h	...
20 h	...
21 h	...
22 h	...
23 h	...
24 h	...
25 h	...
26 h	...
27 h	...
28 h	...
29 h	...
2A h	...
2B h	...
2C h	...
2D h	...
2E h	...
2F h	...
30 h	...
31 h	...
32 h	...
33 h	...
34 h	...
35 h	...
36 h	...
37 h	...
38 h	...
39 h	...
3A h	...
3B h	...
3C h	...
3D h	...
3E h	...
3F h	...
40 h	...
41 h	...
42 h	...
43 h	...
44 h	...
45 h	...
46 h	...
47 h	...
48 h	...
49 h	...
4A h	...
4B h	...
4C h	...
4D h	...
4E h	...
4F h	...
50 h	...
51 h	...
52 h	...
53 h	...
54 h	...
55 h	...
56 h	...
57 h	...
58 h	...
59 h	...
5A h	...
5B h	...
5C h	...
5D h	...
5E h	...
5F h	...
60 h	...
61 h	...
62 h	...
63 h	...
64 h	...
65 h	...
66 h	...
67 h	...
68 h	...
69 h	...
6A h	...
6B h	...
6C h	...
6D h	...
6E h	...
6F h	...
70 h	...
71 h	...
72 h	...
73 h	...
74 h	...
75 h	...
76 h	...
77 h	...
78 h	...
79 h	...
7A h	...
7B h	...
7C h	...
7D h	...
7E h	...
7F h	...

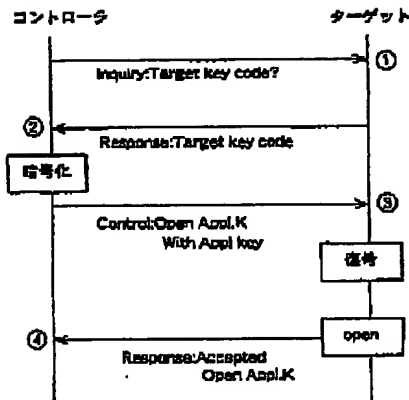
【図10】

10 h	00 h	00 h	55 h	78 h
(Appl. ID)	(open/close)	(close)	(Application key code)	

(9)

特開平9-44354

【図5】



【図6】

OPR4	OPR5	OPR6	OPR7	..
Application No	Application 等に定めた OPC	Application 等に定めた OPR1	Application 等に定めた OPR2	

【図9】

10k h (Appl. K)	80 h (open/close)	FF h (dummy)	58 h (Application key code)	78 h
--------------------	----------------------	-----------------	--------------------------------	------

(a) Status Inquiry Command

10k h (Appl. K)	80 h (open/close)	01 h (open)	58 h (Application key code)	78 h
--------------------	----------------------	----------------	--------------------------------	------

(b) Response Accepted

【図7】

OPR4	OPR5	OPR6	OPR7	OPR8
10k h (Appl. K)	10 h (Target key)	71 h (Value Inq)	FF h (dummy)	FF h (dummy)

(a) Status Inquiry Command

10k h (Appl. K)	10 h (Target key)	71 h (Value Inq)	12 h (Target key code)	34 h
--------------------	----------------------	---------------------	---------------------------	------

(b) Response Stable

10k h (Appl. K)	10 h (Target key)	71 h (Value Inq)	FF h (dummy)	FF h (dummy)
--------------------	----------------------	---------------------	-----------------	-----------------

(c) Response Not Implemented

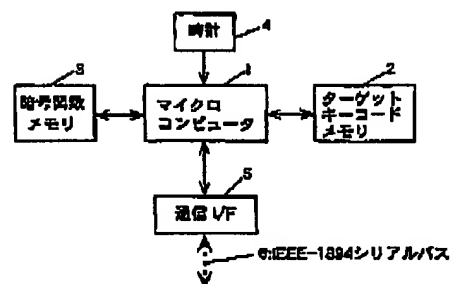
【図11】

Application No	使用権を持っている会社のCompany id
1	xxxxxxh, yyyyyyh
2	xxxxxxh, yyyyyyh
:	:
K	xxxxxxh, yyyyyyh
:	:

【図12】

Target key code	Application key code
1234 h	5878 h
0088 h	0041 h
3333 h	8899 h
:	:

【図13】



【図8】

10k h (Appl. K)	80 h (open/close)	01 h (open)	58 h (Application key code)	78 h
--------------------	----------------------	----------------	--------------------------------	------

(a) Control Command

10k h (Appl. K)	80 h (open/close)	01 h (open)	58 h (Application key code)	78 h
--------------------	----------------------	----------------	--------------------------------	------

(b) Response Accepted

10k h (Appl. K)	80 h (open/close)	01 h (open)	58 h (Application key code)	78 h
--------------------	----------------------	----------------	--------------------------------	------

(c) Control Command

10k h (Appl. K)	80 h (open/close)	01 h (open)	58 h (Application key code)	78 h
--------------------	----------------------	----------------	--------------------------------	------

(d) Response Accepted

(10)

特開平9-44354

フロントページの続き

(51) Int. Cl. 6

H04N 7/167

識別記号

庁内整理番号

F I

H04N 7/167

技術表示箇所

Z